


Procedure No. C-04	SUNY College at Old Westbury  Information Security Program	Policy Summary
--------------------	---	----------------

This is a principle, rather than a rule based policy. It presents guidelines for the campus community to follow when deciding how to handle information considered legally sensitive.¹ A separate implementation guide will be made available for departments to address the mechanics necessary to carry out this policy. In collecting, assembling, reporting, retaining and disposing of legally sensitive information, the College will:

- I. COLLECT only the information that is required under the relevant laws or regulations.² If we don't have the information, we can't lose or compromise it.
- II. SHARE the information only with the people and systems necessary to perform the tasks. The fewer people and places that have the information, the fewer opportunities for it to be compromised.
- III. RETAIN the information for as long as legally or operationally necessary, but no longer. If we don't have it, we can't lose it.
- IV. ENCRYPT information that is transferred from central information systems to local storage so that if a device is lost, stolen or otherwise compromised, the data cannot be recovered without use of a secret key. If paper records are used, equivalent physical access control systems will be maintained.

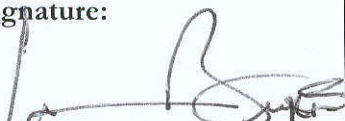
The following categories will be integral parts of the College's Information Security Program:

- I. CLASSIFICATION: Information and systems, physical asset locations and descriptions, will be properly classified into clearly delineated groupings, each requiring its own level of clearance to access.
- II. INVENTORY: A campus wide inventory of such information will be produced resulting in a list of all information and their classification level.
- III. RISK ASSESSMENT: An analysis of the risks to the information in the inventory and appropriate recommendations will be made as to safeguards with the highest classification level receiving the most protection.
- IV. RESTRICTED ACCESS: Individuals can only access information to which they have been granted clearance.
- V. PERFORMANCE DRIVEN: Access policies and clearance levels are integrated into individual employees' performance programs with a master list maintained by human resources.
- VI. INTERNAL CONTROLS: The Information Security Program is integrated into the internal control policies of each division.
- VII. TRAINING: Each division shall engage in periodic training and awareness activities to ensure that all members are aware of and remain in compliance with the College's Information Security Program.

This policy will be updated, procedures developed and compliance will be reviewed annually.

¹ The term *legally sensitive information* encompasses contractually and legally protected non-public College information or data which the College is obliged to treat as confidential whether it is research, clinical, educational or administrative. An example of contractually-protected data would be credit card numbers. Examples of legally-protected data include: Social Security number; Birth date; Home phone number; Home address; Health information; Student data; Ethnicity; and Citizenship.

² Currently, the following laws and regulations govern this policy: NYS Privacy Protection Law; NYS Freedom of Information Act (FOIL); NYS Governmental Accountability, Audit and Internal Control Act; NYS Disposal of Personal Records Law; NYS Information Security Breach and Notification Act; Federal Health Insurance Portability and Accountability Act (HIPAA); Federal Family Educational Rights and Privacy (FERPA); Federal Gramm-Leach-Bliley Act (GLBA); Payment Card Industry Data Security Standards.(PCI-DSS).

Issued By: Dr. Calvin O. Butts, III President, College at Old Westbury	Signature: 	Effective Date: March 13, 2008
---	---	---